

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-298942

(43)Date of publication of application : 24.10.2000

(51)Int.Cl.

G11B 20/10

G06F 3/06

G06F 12/14

G11B 19/02

G11B 19/12

(21)Application number : 11-108173

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 15.04.1999

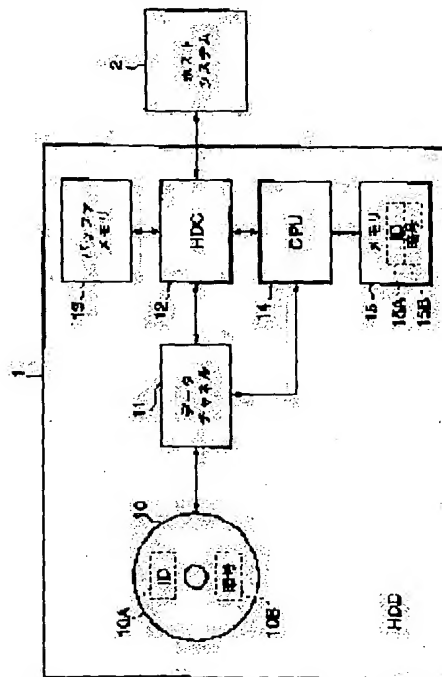
(72)Inventor : KONISHI KAZUO
KATAGIRI TAKAHITO
AWAZU KOICHI

(54) DISK STORAGE DEVICE AND COPY PREVENTING SYSTEM APPLIED TO THIS DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain a disk storage device and a system using this device which have an effective copy preventing function to realize copyright protection of contents data as the result.

SOLUTION: With respect to an attachable/detachable small-sized HSS 1, ID data 10A peculiar to the device and encryption data 10B are stored in a redundant area (alternate sector) on a disk 10. A CPU 14 reads out ID data 10A and encryption data 10B from the disk 10 in accordance with a specific command from a host system 2 and transfers them. The host system 2 uses received data 10A and 10B to encipher contents data and preserves it in the HDD 1.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-298942

(P2000-298942A)

(43) 公開日 平成12年10月24日 (2000. 10. 24)

(51) Int.Cl. ⁷	識別記号	F I	ターミナル (参考)
G 1 1 B 20/10		G 1 1 B 20/10	H 5 B 0 1 7
			F 5 B 0 6 5
G 0 6 F 3/06	3 0 4	G 0 6 F 3/06	3 0 4 M 5 D 0 4 4
			3 0 4 K 5 D 0 6 6
12/14	3 2 0	12/14	3 2 0 E

審査請求 未請求 請求項の数 9 O L (全 8 頁) 最終頁に続く

(21) 出願番号 特願平11-108173

(22) 出願日 平成11年4月15日 (1999. 4. 15)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 小西 和夫

東京都港区芝浦一丁目1番1号 株式会社
東芝本社事務所内

(72) 発明者 片桐 孝人

東京都港区芝浦一丁目1番1号 株式会社
東芝本社事務所内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

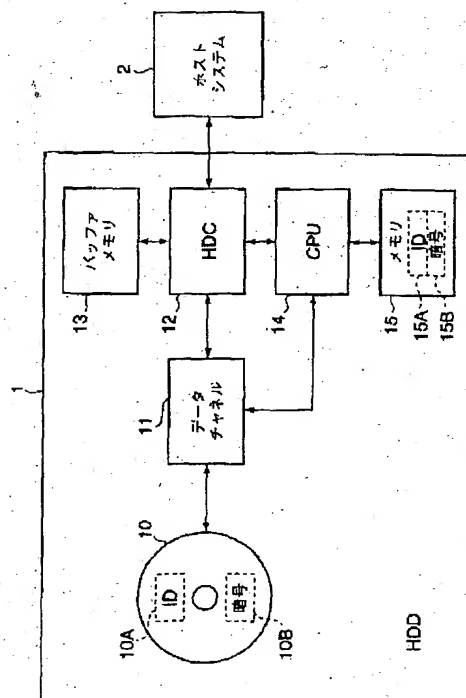
最終頁に続く

(54) 【発明の名称】 ディスク記憶装置及び同装置に適用するコピー防止システム

(57) 【要約】

【課題】 有効なコピー防止機能を有し、結果的にコンテンツデータの著作権保護を実現できるディスク記憶装置及び同装置を利用したシステムを提供することにある。

【解決手段】 着脱可能な小型のHDD 1において、ディスク10上の冗長領域（代替セクタ）に装置固有のIDデータ10A及び暗号データ10Bが記憶されている。CPU 14は、ホストシステム2からの特定コマンドに応じて、ディスク10からIDデータ10A及び暗号データ10Bを読み出して転送する。ホストシステム2は、受信した各データ10A、10Bを利用して、コンテンツデータを暗号化してHDD 1に保存する。



【特許請求の範囲】

【請求項1】 ユーザデータの記録領域、及び当該ユーザデータの記録動作では書換え不可能な記録領域であつて固有の識別データが記録された特定の記録領域を有するディスク記憶媒体と、
ホストシステムからの特定コマンドに応じて、前記識別データを前記特定の記録領域から読出して前記ホストシステムに出力する制御手段とを具備したことを特徴とするディスク記憶装置。

【請求項2】 ディスク記憶媒体をデータの記録媒体として使用するディスク記憶装置であつて、
装置固有の識別データを記憶し、前記ディスク記憶媒体とは区別されたメモリ手段と、
ホストシステムからの記録再生用のコマンドに応じて前記ディスク記憶媒体に対するデータの記録再生を制御し、当該ホストシステムからの特定コマンドに応じて前記メモリ手段から前記識別データを読出して前記ホストシステムに出力する制御手段とを具備したことを特徴とするディスク記憶装置。

【請求項3】 ディスク記憶媒体をデータの記録媒体として使用するディスク記憶装置に適用するコピー防止システムであつて、
前記ディスク記憶媒体または前記ディスク記憶媒体とは区別されたメモリ手段に記憶された装置固有の識別データの読出し動作を制御する制御手段と、
前記制御手段を介して読出した前記識別データを使用して、前記ディスク記憶媒体に記録するコンテンツデータを暗号化するための暗号化キーデータを生成する暗号データ生成手段とを具備したことを特徴とするコピー防止システム。

【請求項4】 前記暗号化キーデータを使用して、指定のコンテンツデータを暗号化した暗号化データ及び当該暗号化キーデータを前記ディスク記憶媒体に記録する記録手段を有することを特徴とする請求項3記載のコピー防止システム。

【請求項5】 前記ディスク記憶媒体から記録されたデータを読出して、所定の出力形態に再生出力する再生手段を有し、
前記再生手段の再生出力時に、前記ディスク記憶媒体から前記暗号化キーデータ及び再生対象のコンテンツデータに対応する暗号化データを読出し、前記暗号化キーデータを使用して当該暗号化データを復号化する復号化手段を備えていることを特徴とする請求項3記載のコピー防止システム。

【請求項6】 前記識別データは装置固有の識別コードを示すと共に、前記ディスク記憶媒体に記録するデータの暗号化処理に必要な暗号データの記憶位置を示し、
前記ホストシステムは、前記制御手段により読出された識別データに基づいて前記暗号データを取得して、前記ディスク記憶媒体に記録するデータを暗号化するための

暗号化キーデータを生成することを特徴とする請求項1又は請求項2記載のディスク記憶装置。

【請求項7】 前記識別データは装置固有の識別コードを示すと共に、前記ディスク記憶媒体に記録するデータの暗号化処理に必要な暗号データの記憶位置を示し、
前記暗号データ生成手段は、前記識別データを使用して前記暗号データを取得し、当該暗号データを使用して前記暗号化キーデータを生成することを特徴とする請求項3記載のコピー防止システム。

【請求項8】 前記ディスク記憶媒体に対するデータの記録を禁止するためのライトプロテクト手段を有することを特徴とする請求項1又は請求項2記載のディスク記憶装置、あるいは請求項3記載のコピー防止システム。

【請求項9】 ディスク記憶媒体をデータの記録媒体として使用するディスク記憶装置であつて、
前記ディスク記憶媒体又は前記ディスク記憶媒体とは区別されたメモリ手段に記憶された装置固有の識別データを、ホストシステムからの特定コマンドに応じて読出手段と、
前記読出し手段により読出した前記識別データを使用して、前記ディスク記憶媒体に記録するコンテンツデータを暗号化する暗号化機能を含むセキュリティ処理を実行するセキュリティ機能手段とを具備したことを特徴とするディスク記憶装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えば映像や音声などの情報コンテンツを記録するディスク記憶装置に関し、特に当該情報コンテンツのコピーを防止するための機能を有するディスク記憶装置または当該装置を利用したシステムに関する。

【0002】

【従来の技術】近年、コンピュータデータだけでなく、映像や音声（特に音楽）などの情報コンテンツをデジタル化したデータ（コンテンツデータと表記する）を記憶する媒体として、高速アクセス及び大容量化が可能な小型のハードディスクドライブ（HDD）が注目されている。HDDは、記憶媒体であるディスクとドライブ機構とが一体的に構成された構造が特徴である。特に小型のHDDは、パーソナルコンピュータの内蔵型記憶装置だけでなく、デジタルテレビやデジタルカメラ（ビデオカメラ及びスチールカメラ）などの記憶媒体として適用範囲が広がっている。

【0003】ところで、コンテンツデータは、デジタル放送、インターネット、または記録メディアなどを利用した配信や流通により、不特定多数のユーザに提供されることが一般的である。このため、コンテンツデータの取り扱いでは、著作権保護、端的にはコピー防止機能が重要である。

【0004】

【発明が解決しようとする課題】前述したように、デジタルのコンテンツデータは、インターネットやパーソナルコンピュータなどを利用して、コピーが容易である。このため、近年では、各種の記録メディア、コンピュータシステム、ネットワークなどの技術開発と関連して、コピー防止技術の開発が推進されている。しかしながら、コンテンツデータの記憶媒体としてHDDを利用した装置やシステムでは、必ずしも適当で有効なコピー防止機能が開発されていない。

【0005】そこで、本発明の目的は、有効なコピー防止機能を有し、結果的にコンテンツデータの著作権保護を実現できるディスク記憶装置及び同装置を利用したシステムを提供することにある。

【0006】

【課題を解決するための手段】本発明の第1の観点は、通常のユーザデータの記録動作では、書き換え不可能なディスクの記録領域または内部メモリに、予め装置固有の識別データが記憶されたディスク記憶装置である。具体的には、識別データは、ディスク上でユーザデータの記録領域以外の冗長領域（代替セクタ）、または装置内部に設けられた制御情報を記憶するための不揮発性で書き換え可能なICメモリ（EEPROM）に記憶される。更に、本装置は、パーソナルコンピュータなどのホストシステムから特定コマンドを受信すると、当該識別データを記録領域から読出して出力する機能を有する。

【0007】このような構成であれば、ホストシステムは、映像や音声などのコンテンツデータをディスク記憶装置に記録する場合に、識別データを読出すことにより、当該装置を識別できる。従って、ホストシステムは、コンテンツデータを記録したディスク記憶装置を管理できるため、結果的に当該コンテンツデータに対する無制限なコピーを防止する機能を実現できる。

【0008】本発明の第2の観点は、前記のような装置固有の識別データを記憶したディスク記憶装置とホストシステムとを有するコピー防止システムである。本システムは、ディスク記憶装置に記憶された識別データを使用して、ディスク記憶媒体に記録するコンテンツデータを暗号化するための暗号化キーデータを生成する暗号データ生成手段を備えている。

【0009】このような構成であれば、ディスク記憶装置毎にコンテンツデータを暗号化して記録することができるため、当該ディスク記憶装置を別のホストシステムがアクセスした場合に、記録したコンテンツデータの再生を防止することが可能となる。従って、結果的にディスク記憶装置に記録したコンテンツデータに対する無制限なコピーを防止する機能を実現できる。

【0010】

【発明の実施の形態】以下図面を参照して、本発明の実施の形態を説明する。

【0011】図1は同実施形態に係るHDDの要部

を示すブロック図であり、図2は同実施形態に係るコピー防止システムを説明するための概念図である。

【0012】（HDDの構成）同実施形態のHDD1は、例えばカード型でホストシステム2に対して着脱可能なリムーバブル（removal）型の小型ディスクドライブを想定する。HDD1は、カード型の筐体の内部に、記憶媒体であるディスク10およびドライブ機構が一体的に設けられた構造である。ドライブ機構は主として、ディスク10を回転させるスピンドルモータや、当該ディスク10に対してデータのリード/ライト動作を実行するためのヘッドをシークさせるアクチュエータからなる（図示せず）。

【0013】HDD1は、ディスク10及びドライブ機構以外に、データの記録再生及びデータ転送を処理するための制御・信号処理系を有する。制御・信号処理系は、データチャネル11と、ディスクコントローラ（HDC）12と、バッファメモリ13と、マイクロプロセッサ（CPU）14と、メモリ15とを有する。データチャネル11は、ヘッドによりディスク10に記録すべきデータ信号及びディスク10から読出されたデータ信号に対する各種の信号処理を実行する。HDC12は、HDD1とホストシステム（同実施形態ではパーソナルコンピュータを想定する）2とのインターフェースを構成し、主としてデータ転送機能を有する。バッファメモリ13は、HDC12により制御されて、ディスク10から読出されたデータ（再生データ）及びホストシステム2から転送されたデータ（記録データ）を一時的に保存する。

【0014】CPU14は、HDD1のメイン制御装置であり、同実施形態のコピー防止機能に係る制御動作を実行する。メモリ15は、CPU14により制御されるICメモリであり、通常では書き換え可能な不揮発性メモリ（例えばEEPROM）からなる。

【0015】同実施形態のHDD1では、ディスク10上の特定の記録領域に、IDデータ10A及び暗号データ10Bが予め記憶されている。特定の記録領域とは、通常のユーザデータ（後述するコンテンツデータやコンピュータデータ）の記録動作では書き換え不可能（アクセス不可）な代替セクタ（冗長記録領域）を想定する。IDデータ10Aは、装置固有の識別コード及び暗号データ10Bのアドレスを示す識別データである。また、暗号データ10Bは、後述するように、ホストシステム2側でコンテンツデータの暗号化処理に必要な暗号化キーデータを生成するために使用するデータである。

【0016】なお、IDデータ10A及び暗号データ10Bは、EEPROM15に記憶されていてもよい。CPU14は、ホストシステム2からHDC12を介して、特定コマンドを受信すると、ディスク10またはメモリ15からIDデータ10A及び暗号データ10Bを読出してホストシステム2に転送する。

【0017】（コピー防止システム）同実施形態では、図2に示すように、映像や音声などの情報コンテンツをデジタル化したコンテンツデータを、サーバ3からインターネット4を介してパーソナルコンピュータ（P.C）2に提供されるシステムを想定する。サーバ3は、コンテンツデータを暗号化キーデータ（共通キー）により暗号化し、当該暗号化データ3B及び当該暗号化キーデータを含むセキュリティ情報3Aを送信する。

【0018】PC2は、インターネット4から送信された暗号化データ3B及びセキュリティ情報3Aをダウンロードし、後述するような手順により、内部に装着したHDD1にコピーする。なお、セキュリティ情報3Aには、コピーを1回だけ許可するコピー制限情報も含まれている。

【0019】このようなシステムにおいて、図1と図2と共に図4のフローチャートを参照して、HDD1へのコピー動作（コンテンツデータの記録動作）を説明する。

【0020】まず、PC2は、HDD1に対して、IDデータ10Aを読み出すための特定コマンド（IDデータ10Aのアドレスを含む）を発行する。CPU14は、特定コマンドの受信に応じて、ディスク10の特定記録領域からIDデータ10Aを読み出して、PC2に転送する（ステップS1）。なお、メモリ15からIDデータ10Aを読み出す場合も同様である。

【0021】PC2は、受信したIDデータ10Aを使用して、HDD1がセキュリティ機能が設けられている記憶媒体であることを認証する。更に、PC2はIDデータ10Aを使用して、暗号データ10Bのアドレスを算出し、このアドレスを含む特定コマンドを発行する（ステップS2）。CPU14は、特定コマンドの受信に応じて、ディスク10の特定記録領域から暗号データ10Bを読み出して、PC2に転送する（ステップS3）。

【0022】PC2は、HDD1固有の暗号データ10Bを取得すると、当該暗号データ10B及びダウンロードしたセキュリティ情報3Aを使用して、暗号化キーデータ10Cを生成する（ステップS4）。PC2は、生成した暗号化キーデータ10CをHDD1に転送し、ディスク10上の特定記録領域（代替セクタ）またはメモリ15の指定領域に記録する（ステップS5）。この場合、暗号化キーデータ10Cの記録アドレスは、HDD1固有の暗号データ10Bに基づいて設定される。

【0023】次に、PC2は、生成した暗号化キーデータ10Cを使用して、ダウンロードしたコンテンツデータ（共通キーによる暗号化データ）3Bを暗号化して、HDD1に転送する（ステップS6）。HDD1は、通常のユーザデータと同様に、暗号化したコンテンツデータ10Dをディスク10上の記録領域に記録する（ステップS7）。

【0024】以上の処理により、PC2は、サーバ3から取得したコンテンツデータを暗号化して、HDD1にコピーする。PC2は、サーバ3からのセキュリティ情報3Aに基づいて、1回目のコピーが終了後に2回目以降のコピーを禁止するためのロック処理を実行する。

【0025】（再生システム）次に、図3及び図5のフローチャートを参照して、同実施形態の再生システムを説明する。

【0026】前述したように、PC2により、HDD1には暗号化されたコンテンツデータ10Dが記録されている。ここで、PC2からHDD1を取出して、図3に示すように、再生プレーヤ5に接続するシステムを想定する。再生プレーヤ5は、HDD1から読出したコンテンツデータから、映像信号や音声信号を再生して例えばデジタルテレビなどの再生出力装置51に出力する。

【0027】再生プレーヤ5は、HDD1が接続されて再生動作が開始されると、HDD1からIDデータ10Aを読み出す（ステップS10）。ここで、再生プレーヤ5のCPUが、前述のPC2と同様に、特定コマンド（IDデータ10Aのアドレスを含む）を発行して、ディスク10の特定記録領域からIDデータ10Aを読み出す。このIDデータ10Aを使用して、再生プレーヤ5のCPUは、HDD1がセキュリティ機能が設けられている記憶媒体であることを認証する。

【0028】さらに、再生プレーヤ5は、受信したIDデータ10Aを使用して、暗号データ10Bのアドレスを算出し、HDD1から当該暗号データ10Bを読み出す（ステップS11、S12）。再生プレーヤ5は、取得した暗号データ10Bに基づいて、暗号化キーデータ10Cのアドレスを算出し、HDD1から当該暗号化キーデータ10Cを読み出す（ステップS13、S14）。

【0029】再生プレーヤ5は、内蔵している復号化処理部（専用回路またはCPUの機能）50により、読出した暗号化キーデータ10Cを使用して、HDD1に記録されているコンテンツデータ（暗号化データ）10Dを復号化して、元のコンテンツデータに再生する（ステップS15、S16）。再生出力装置51は、再生された映像をディスプレイ上に表示出力し、スピーカから再生された音声を出力する。

【0030】以上のように同実施形態のシステムであれば、HDD1の固有のIDデータ及び暗号データを利用して暗号化したコンテンツデータを、HDD1に記録することになる。従って、仮にHDD1を別のHDDや記録メディアにコピーする場合に、当該HDD1に対応するPC2や、セキュリティ機能が設けられた特別の再生プレーヤ5は、HDD1から固有のIDデータを認証しないと、暗号データを読み出すことはできないため、コピーをしても再生できない。これにより、HDD1に記録したコンテンツデータを、他のHDDや記録メディアでは再生することを防止できるため、結果的に当該コンテ

ンツデータの著作権の保護を実現することが可能となる。

【0031】なお、同実施形態では、インターネットから予め暗号化されたコンテンツデータ（著作権が保護されたデータ）を、HDD1にダウンロードする場合を想定したが、これに限らず、デジタル放送や他の記録メディアからコピーされた場合でも適用できる。

【0032】（変形例1）図6は、同実施形態の変形例を示すブロック図である。即ち、本変形例は、前述した同実施形態のコピー防止機能を、CPUではなく、専用のセキュリティ・チップ（メモリを内蔵したIC）61を内蔵したHDD60である。

【0033】本HDD60では、セキュリティ・チップ61は予めIDデータ10A及び暗号データ10Bを記憶し、HDC62を介して入力されたホストシステム2からの特定コマンドに応じて当該IDデータ10A及び暗号データ10Bをホストシステム2に転送する機能を備えている。なお、コピー防止機能の動作は、前述の同実施形態の場合と同様であるため、説明を省略する。

【0034】このような本変形例の方式であれば、HDDのCPUの負担を軽減し、ディスク10上の特定記録領域に対するアクセスを不要にできる。また、セキュリティ・チップ61には、同実施形態に係るコピー防止機能以外のセキュリティ機能を含ませることも容易である。具体的には、例えばコンテンツを供給するサーバと連動して、1週間毎に暗号データを変更するなどの機能である。また、IDデータ10A及び暗号データ10Bを、セキュリティ・チップ61及びディスク10の双方に記憶させることにより、セキュリティ機能の効果を高めることが可能となる。

【0035】（変形例2）図7及び図8は、同実施形態のHDD1において、いわゆるライトプロテクト機能を有する変形例に関する。

【0036】即ち、本変形例のHDD70は、図7に示すように、カード型筐体（例えばPCMCIA規格）の中にディスク、ドライブ機構及び制御・信号処理系を内蔵しており、その外側にライトプロテクト用スイッチ（例えばスライドスイッチ）71を有する。また、筐体の外側には、通常ではパーソナルコンピュータなどのホストシステムに接続するためのコネクタが設けられている。さらに、図8を参照して、ライトプロテクト機能を説明する。

【0037】ライトプロテクト用スイッチ71がオン（即ち、ライトプロテクト機能の有効を意味する）されると、HDD70の内部に設けられたラッチ回路73がその情報（ライトプロテクト）をラッチする。ホストシステム2は、コネクタ72によりHDD70に接続すると、ライトプロテクト機能のオン／オフを確認するためのコマンドを発行する。

【0038】HDD70では、内部ロジック（HDC及

びCPUの各機能）74がホストシステム2からのコマンドに応じて、ラッチ回路73のクロック入力にクロックパルスを供給して、当該ラッチ回路73から情報を読出す。そして、内部ロジック（HDC及びCPUの各機能）74は、読出した情報をコネクタ72を介してホストシステム2に出力する。ホストシステム2は、受信した情報に基づいて、ライトプロテクト機能が有効であるか否かを識別する。

【0039】以上のようなライトプロテクト機能を有するHDDであれば、ユーザがスイッチ71を操作するだけで、HDDのディスクに対するデータの書き込み動作を禁止できる。従って、特にカード型などの着脱可能なHDDにおいて、記録したデータを保存したい場合に、ライトプロテクト機能を有効にすれば、保存データを確実に保護することが可能となる。これにより、当該HDDを、従来の映像や音声を保存する記録メディアとして使用することが可能となる。

【0040】なお、同実施形態及び各変形例は、ディスク記憶装置としてHDDを想定したが、他のディスク記憶媒体である書き込み可能な光ディスク装置や光磁気ディスク装置にも適用することが可能である。

【0041】

【発明の効果】以上詳述したように本発明によれば、第1にディスク記憶媒体に記録するコンテンツデータの無制限なコピーを確実に防止する機能を備えたディスク記憶装置及び同装置を適用したシステムを提供することができる。従って、特にディスク記憶装置として着脱可能な小型の装置に適用すれば、有効なコピー防止機能により、結果的にコンテンツデータの著作権保護を実現することができる。第2に、ライトプロテクト機能を有するディスク記憶装置を実現することにより、保存データを確実に保護できる。従って、特に着脱可能な小型のディスク記憶装置に適用すれば、コンテンツデータを保存するための記録メディアとして使用することが可能となる。

【図面の簡単な説明】

【図1】本発明の実施形態に係るHDDの要部を示すブロック図。

【図2】同実施形態に係るコピー防止システムを説明するための概念図。

【図3】同実施形態に係るデータ再生系を説明するための概念図。

【図4】同実施形態に係るデータ記録動作を説明するためのフローチャート。

【図5】同実施形態に係るデータ再生動作を説明するためのフローチャート。

【図6】同実施形態の変形例1に係るHDDの要部を示すブロック図。

【図7】同実施形態の変形例2に係るHDDの外観を説明するための図。

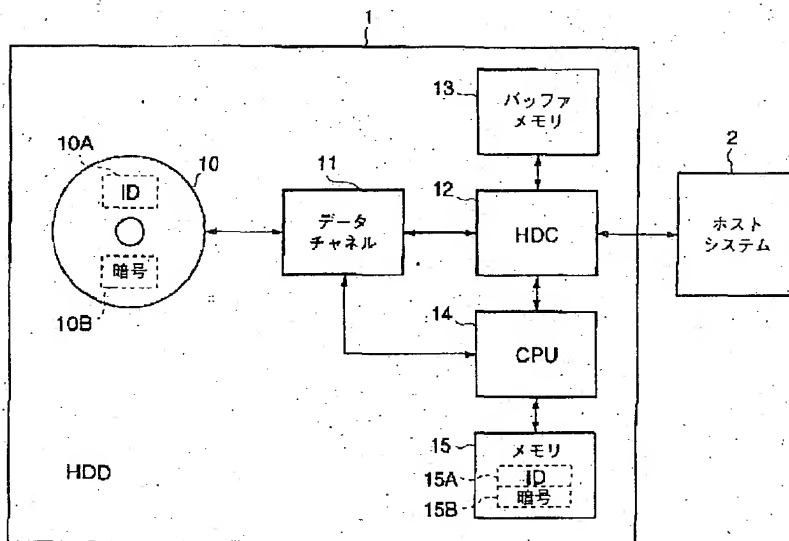
【図8】同変形例2に関するHDDの内部構成を説明するための図。

【符号の説明】

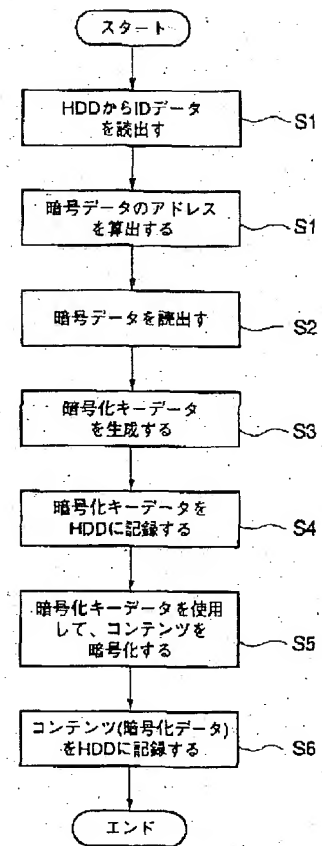
- 1…ディスク記憶装置 (HDD)
2…ホストシステム (パーソナルコンピュータ)
3…サーバ
4…インターネット
5…再生プレーヤ
10…ディスク

- 11…データチャンネル
12…ディスクコントローラ (HDC)
13…バッファメモリ
14…マイクロプロセッサ (CPU)
15…メモリ (EEPROM)
50…復号化処理部
51…再生出力装置
61…セキュリティ・チップ
71…ライトプロテクトスイッチ

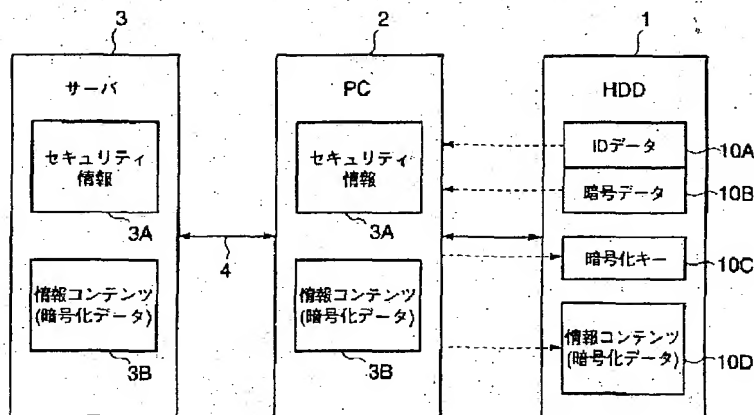
【図1】



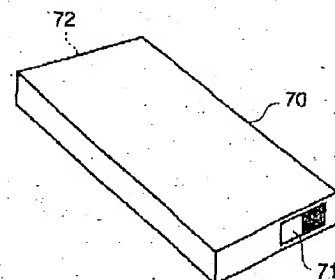
【図4】



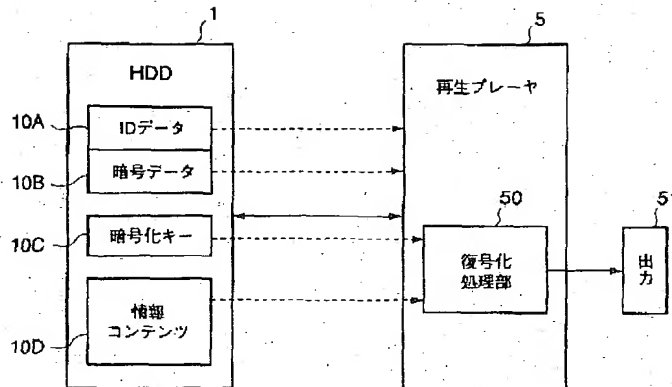
【図2】



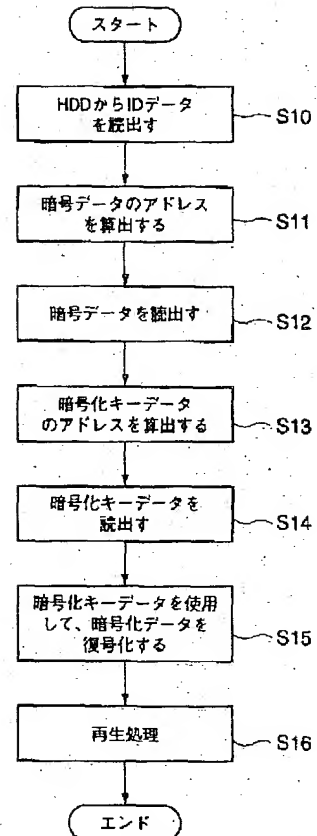
【図7】



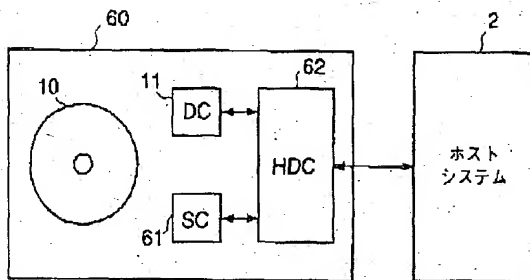
【図 3】



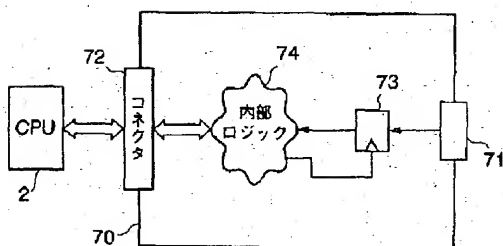
【図 5】



【図 6】



【図 8】



フロントページの続き

(51)Int.Cl.⁷G 1 1 B 19/02
19/12

識別記号

5 0 1
5 0 1

F I

G 1 1 B 19/02
19/12

テマコード (参考)

5 0 1 Q
5 0 1 K

(72)発明者 栗津 浩一

東京都港区芝浦一丁目1番1号 株式会社
東芝本社事務所内

F ターム(参考) 5B017 AA02 AA06 BA05 BA07 CA07
CA12 CA14 CA16
5B065 BA01 CA11 PA02 PA04 PA16
5D044 BC01 CC04 DE49 DE50 FG10
FG18 GK17 HL01 HL08 HL11
5D066 EA02 EA13 EA17 EA21 EA22
HA01